IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

OCLC, Inc. **Plaintiff,** **v.** **ANNA'S ARCHIVE, f/k/a PIRATE LIBRARY MIRROR, et al.,** **Defendants.**	**Case No. 2:24-cv-00144-MHW-EDP** **Judge Michael H. Watson** **Magistrate Judge Elizabeth A. Preston Deavers**

PLAINTIFF OCLC, INC.'S ADDITIONAL MEMORANDUM IN SUPPORT OF ITS MOTION FOR DEFAULT JUDGMENT AGAINST DEFENDANT ANNA'S ARCHIVE

Pursuant to this Court's September 19, 2024 Order (Dkt. 42) ("Order"), Plaintiff OCLC, Inc. ("OCLC") files this Additional Memorandum in Support of its Motion for Default Judgment Against Defendant Anna's Archive, f/k/a Pirate Library Mirror ("Anna's Archive"). In its Order, the Court directed OCLC to explain "which claims it seeks default judgment on and why, as a matter of law, the facts it has pled in its complaint are sufficient to establish Anna's Archive's liability for each such claim" in light of the "complex and developing area of law" regarding the "legal proprietary of data harvesting." Order, Dkt. 42 at PageID 822. OCLC's Motion for Default Judgment Against Anna's Archive ("Motion") (Dkt. 40) focused on the appropriate amount of damages and availability of injunctive relief for OCLC. OCLC appreciates the opportunity provided by the Court to demonstrate why its well-pled factual allegations support an entry of judgment as to liability against Anna's Archive.

OCLC addresses the Court's concerns as follows. ***First***, the current body of caselaw addressing data harvesting under federal law poses no obstacle to this Court's granting OCLC's

Motion. In fact, *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022), which this Court cited in its Order, demonstrates that OCLC's claims lie against Anna's Archive and that Anna's Archive's actions at issue in this case are improper. ***Second***, the allegations in OCLC's Complaint establish liability against Anna's Archive for all claims—with many of the supporting facts coming directly from Anna's Archive's own admissions. Furthermore, William Rozek's and Barton Murphy's declarations, which OCLC submitted in this case, provide factual support for these well-pled allegations.

I. Factual Background

Beginning in fall 2022, Anna's Archive attacked WorldCat.org and OCLC's servers, which significantly effected OCLC's operations and networks. Compl. ¶¶ 9, 75; William Rozek Decl., ¶¶ 38, 44–57, Dkt. 40-1. Anna's Archive's attacks and hacking took three forms.[1] First, Anna's Archive used bots to run a script on the public user interface of WorldCat.org, harvesting, or scraping, both publicly accessible and enriched WorldCat data from OCLC. Compl. ¶¶ 76–77; Barton Murphy Decl., ¶ 10, Dkt. 30-1. Second, Anna's Archive used bots to directly call or "ping" OCLC's servers, thereby tricking OCLC's servers and effectively bypassing the public user interface of WorldCat.org. *See* Compl. ¶ 78; Murphy Decl. ¶ 10. This allowed Anna's Archive to harvest enriched proprietary, non-public data directly from OCLC's servers. Compl. ¶ 78; Murphy Decl. ¶ 10. Third, Anna's Archive misappropriated an OCLC member library's credentials to harvest enriched proprietary, non-public data through a subscription-based variation of WorldCat.org that is only available to paid subscribers. Compl. ¶¶ 79–80. Anna's Archive made all these data available for mass download to encourage and support its overarching piracy aims

[1] Here, OCLC focuses on Anna's Archive's hacking and data harvesting or scraping conduct. OCLC incorporates by reference the background section of its initial Motion (Dkt. 40), along with the facts alleged in its Complaint (Dkt. 1).

in violation of international and federal law. *E.g.*, *id.* ¶¶ 93–95; Rozek Decl. ¶¶ 40, 61; Murphy Decl. ¶ 10.

Importantly, Anna's Archive hacked, scraped, and distributed OCLC WorldCat data, much of which was proprietary, non-public information. To support OCLC's continuous investment in developing, maintaining, and enhancing WorldCat data, member libraries must join the OCLC collective, *i.e.*, subscribe to WorldCat. Compl. ¶¶ 36–40. This allows OCLC and members to share in the benefits and costs of maintaining WorldCat. *Id.* ¶ 41. OCLC's WorldCat Rights and Responsibilities for the OCLC Cooperative demonstrate that WorldCat data is primarily a collective good—not a public good. *See id.* ¶¶ 42–45; *see also* WorldCat Rights & Responsibilities for the OCLC Cooperative, Dkt. 1-1. OCLC's WorldCat.org Services Terms and Conditions ("Terms and Conditions") further protect the value of the collective good—the proprietary, enhanced WorldCat data—by providing specific, additional protections to the limited WorldCat data that is offered to the public via WorldCat.org. *See* Terms & Conditions, Dkt. 1-2.

Anna's Archive illegally hacked and scraped OCLC's data and servers and distributed that data *en masse* in violation of Ohio contract, tort, and statutory law. For example (and as described in greater detail below), the Terms and Conditions expressly prohibit WorldCat.org users from harvesting, distributing, displaying, disclosing, or storing material amounts of WorldCat data. Compl. ¶¶ 122–27; Rozek Decl. ¶ 32. Moreover, Anna's Archive's hacking and scraping violates Ohio law, which prohibits gaining access to a computer system and computer network beyond the scope of express consent (here, OCLC's Terms and Conditions). Compl. ¶¶ 168–73. By hacking, scraping, and giving away OCLC's WorldCat data for free, Anna's Archive also tortiously interfered with OCLC's contracts and prospective customers, *id.* ¶¶ 135–42, 151–58, as well as committed other torts described below, *see infra*, Part III.

II. Cases Addressing Data Harvesting under Federal Law Are Inapplicable.

This is not a website scraping case under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) ("CFAA"), and therefore, CFAA cases have no applicability here. Take *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022), for example, which this Court cites in its Order. Order, Dkt. 42 at PageID 822. In *hiQ Labs*, the Ninth Circuit considered whether LinkedIn could prevent a competitor, hiQ Labs, "from collecting and using information that LinkedIn users had shared on their public profiles, available for viewing by anyone with a web browser." 31 F.4th at 1184. When LinkedIn prevented hiQ Labs from scraping LinkedIn data, hiQ Labs sought a declaratory judgment against LinkedIn for tortious interference with contractual relationships. *Id.*; *see also id.* at 1188 (considering whether the plaintiff had demonstrated "serious questions going to the merits" in a preliminary-injunction analysis).

While evaluating whether hiQ Labs had demonstrated a likelihood of success on the merits, the court considered LinkedIn's defense that hiQ Lab's state-law tortious interference claim was preempted by the CFAA. *Id.* at 1194–95. There, "[t]he pivotal CFAA question" was whether hiQ Labs scraped and used "LinkedIn's data 'without authorization' within the meaning of the CFAA." *Id.* at 1195. The Ninth Circuit held that scraping information that is available to all on a public website, such as LinkedIn, is not covered under the CFAA. *Id*. at 1201 ("[W]hen a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA.").

The holding of *hiQ Labs*, a non-binding, out-of-circuit decision, is legally inapplicable to this case for two key reasons. ***First***, this is not a CFAA case; OCLC has not asserted a CFAA claim against Anna's Archive, nor does it point to the CFAA as a defense (as the defendant did in *hiQ Labs*). *hiQ Labs*, which interprets the statutory text of the CFAA, has no bearing on the state-law claims at issue here. In fact, the Ninth Circuit explicitly warned in *hiQ Labs* that its holding

was limited solely to its analysis of the statutory text of the CFAA and reaffirmed that "victims of data scraping are not without resort, even if the CFAA does not apply." *Id.* at 1201. "[S]tate law trespass to chattels claims may still be available . . . [a]nd other causes of action, such as . . . unjust enrichment, conversion, breach of contract . . . may also lie." *Id.* OCLC's claims against Anna's Archive are ***the very same*** state-law causes of action that the Ninth Circuit said "may still be available," independent of the CFAA, to provide protection to victims of data scraping and hacking.

Second, even if *hiQ Labs* were applied more broadly outside the CFAA (which it should not be), Anna's Archive's actions here are factually distinct from the data scraping at issue in *hiQ Labs*.[2] The Ninth Circuit concluded that the "CFAA's prohibition on accessing a computer 'without authorization' is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer." *Id*. However, the data-scraping plaintiff in *hiQ Labs* was not liable under the CFAA because it harvested data from a "computer network [that] generally permits public access to its data" (rather than private data) and data that belonged to LinkedIn users—not the defendant, LinkedIn. *Id.*; *see also id.* at 1199 (distinguishing *Facebook, Inc. v. Power Ventures, Inc*., 844 F.3d 1058 (9th Cir. 2016), because "Facebook . . . tried to limit and control access to its website as to the purposes for which Power Ventures sought to use it").

[2] Other factual differences between *hiQ Labs* and this case are also critical. hiQ Labs was a bona fide data analytics company, while Anna's Archive is a pirate library that admits its scheme infringes upon copyright laws. Compl. ¶ 67. Moreover, LinkedIn permitted hiQ Labs to scrape its data for years, only demanding that hiQ Labs stop when LinkedIn planned to introduce a competing data analytics tool. *hiQ Labs*, 31 F.4th at 1193–94. Here, however, Anna's Archive hacked into OCLC's servers to scrape, harvest, and otherwise gain access to OCLC's proprietary and protected WorldCat data ***and*** to publicly provide it for mass download. Compl. ¶¶ 86, 100–06. And unlike LinkedIn, OCLC also promptly worked to ward off the intrusion. *Id.*

Here, Anna's Archive went beyond accessing information that was already publicly available. True, Worldcat.org is a public website, and Anna's Archive, through its use of bots, scraped and harvested certain WorldCat data that was publicly accessible on Worldcat.org. Compl. ¶¶ 51, 77; Rozek Decl. ¶¶ 38, 39. But Anna's Archive did more than that. Anna's Archive accessed and used the publicly available data in violation of the Terms and Conditions. *See infra*, Part III. There was no comparable agreement providing such contractual protections over the "public" data in *hiQ Labs*.[3]

Anna's Archive also improperly accessed non-public data. *hiQ Labs* recognized that "even computer and servers hosting public websites may contain areas that require authorization to access." *hiQ Labs*, 31 F.4th at 1199 n.17. Such is the case here; Anna's Archive exceeded any authorization from OCLC when it hacked, harvested, and scraped WorldCat.org, as evident not only by its intrusion beyond OCLC's public interface, but also by its violation of OCLC's Terms and Conditions. When an individual searches Worldcat.org, they have a limited view of the WorldCat record (and accompanying data) that was searched for; in fact, most of a WorldCat record's data is unavailable on WorldCat.org because the full record is only available to member libraries as part of a paid subscription. Compl. ¶¶ 6, 52; Rozek Decl. ¶¶ 14, 15. OCLC reserves the full record for subscribers because the main value of its data comes from the modifications,

[3] LinkedIn's User Agreement in *hiQ Labs* is also substantially different than OCLC's Terms and Conditions because the agreement provided that the users owned the content they post on LinkedIn, and LinkedIn is only granted a "non-exclusive license" to "use, copy, modify, distribute, publish, and process" that information. *hiQ Labs*, 31 F.4th at 1185. Accordingly, LinkedIn could not claim any violation of its User Agreement for scraping that occurred after LinkedIn terminated hiQ Lab's user status, nor even the scraping that occurred prior to the letter because LinkedIn knew of the scraping and did not stop it for years. *Id.* at 1194. In contrast, OCLC relies on Terms and Conditions for WorldCat.org, which grants users a limited-use license of its data—including publicly available data. Compl. ¶ 58; Rozek Decl. ¶ 32. OCLC also acted instantly and consistently with its Terms and Conditions.

improvements, and aggregate availability that OCLC provides for cataloging and other library services. Compl. ¶¶ 52, 59. The paid subscriptions are vital to OCLC's business because the more libraries that participate, the more available records, and the more valuable WorldCat becomes for OCLC's members and as a collective good. *Id.* ¶ 101; Rozek Decl. ¶¶ 10, 61.

Anna's Archive hacked and harvested the proprietary, non-public WorldCat data reserved for subscribers by utilizing means more invasive than crawling the public face of WorldCat.org with bots. Compl. ¶¶ 78–79. In *hiQ Labs* parlance, OCLC erected gates around certain areas of its website, computer network, and computer systems, beyond which Anna's Archive trespassed to access and steal protected data only available to paying customers. *See hiQ Labs*, at 1199 (explaining the "gates-up-or-down inquiry," *i.e.*, that "limitations on access" to a website or system constitutes a "gate" and that "[i]f authorization is required and has *not* been given, the gates are down"). Anna's Archive bypassed the public user interface, or search, of Wordcat.org by directly "pinging" OCLC's servers, and was able to pull more fulsome records directly from OCLC's servers. Compl. ¶ 78.

In other words, Anna's Archive went under or around the "gate" to access OCLC's WorldCat data. Anna's Archive admitted that it obtained fuller records because it circumvented OCLC's security features, accessing private data and unauthorized areas. *Id.* ¶ 89 ("Over the past year, we've meticulously scraped all WorldCat records. At first, we hit a lucky break. WorldCat was just rolling out their complete website redesign (in Aug 2022). This included a substantial overhaul of their backend systems, introducing many security flaws. We immediately seized the opportunity, and were able scrape hundreds of millions (!) of records in mere days."). Anna's Archive also harvested the majority of the WorldCat data by hacking into a library member's paid

account and using the member's credentials to pull full WorldCat records that were not otherwise publicly available without a subscription. *Id.* ¶ 79.

Courts interpreting *hiQ Labs* have agreed that when an entity accesses private, non-public data via improper means, this constitutes access without authorization under the CFAA. *See, e.g.*, *Meta Platforms, Inc. v. BrandTotal Ltd*., 605 F. Supp. 3d 1218, 1267 (N.D. Cal. 2022) (defendant hijacked a user's logged-in sessions on Facebook and Instagram and manipulated Meta's servers to access further information); *United States v. Thompson*, No. CR19-159-RSL, 2022 WL 1719221, at *3 (W.D. Wash. May 27, 2022) (defendant used "a technological process that went beyond merely typing the URL into a browser, or a name into Google, as one would access a public LinkedIn profile"); *Ryanair DAC v. Booking Holdings Inc*., No. CV 20-1191-WCB, 2024 WL 3732498, at *7 (D. Del. June 17, 2024) (using stolen credentials to obtain non-public information).

In sum, *hiQ Labs* is both legally and factually distinguishable from this default-judgment case. *hiQ Labs* addresses a federal statute that is not implicated here and considers the proper access of publicly available data, while Anna's Archive hacked, scraped, and harvested OCLC's public data in violation of the Terms and Conditions and OCLC's non-public, proprietary data behind WorldCat.org. Accordingly, *hiQ Labs* and similar federal precedent present no issue to this Court granting default judgment in favor of OCLC on viable state-law claims.

III. The Well-Pled Facts in OCLC's Complaint Support Granting Default Judgment on All Claims Against Anna's Archive.

OCLC's Complaint asserts claims against Anna's Archive for breach of contract, unjust enrichment, tortious interference, violation of Ohio Revised Code § 2913.04, trespass to chattels, conversion, and civil conspiracy. Once again, many of the claims OCLC has brought against Anna's Archive are the very same state-law causes of action that the Ninth Circuit recognized as providing protection to victims of data scraping and hacking in *hiQ Labs*, 31 F.4th at 1201. OCLC

seeks default judgment on all claims, and the facts pled in the Complaint are sufficient to establish Anna's Archive's liability for each claim as a matter of law.

Breach of Contract. OCLC states a claim for contractual breach of the Terms and Conditions against Anna's Archive. *See Asset Mgmt. One LLC v. U.S. Bank Nat'l Ass'n*, 569 F. App'x 438, 441 (6th Cir. 2014) (the elements for a breach of contract claim under Ohio law are "(1) the existence of a contract; (2) performance by the plaintiff; (3) breach by the defendant; and (4) damage or loss to the plaintiff as a result of the breach." (citation omitted)). Anna's Archive breached at least four provisions of the Terms and Conditions, which Anna's Archive agreed to when it accessed WorldCat.org. Compl. ¶ 58; Murphy Decl. ¶ 7; Rozek Decl. ¶ 31. First, it scraped and harvested material amounts of WorldCat data in violation of §3(A)(iv) of the Terms and Conditions. Terms & Conditions, Dkt. 1-2 at PageID 46; *see supra* Part I. Second, it "distribut[ed], display[ed], or disclos[ed]" WorldCat data when it made the data available for mass download and encouraged users to set up torrents to facilitate further distribution in violation of §3(A)(v) Terms & Conditions, Dkt. 1-2 at PageID 46; Compl. ¶¶ 93–94; Rozek Decl. ¶ 32. Third, by maintaining the data on its website, Anna's Archive has engaged in "long-term storage" of WorldCat data violation of §3(A)(vi). Terms & Conditions, Dkt. 1-2 at PageID 46; Compl. ¶¶ 93–94; Rozek Decl. ¶ 32; *see also* ¶ 86 (noting the data has been posted since October 2023). Finally, Anna's Archive violated § 3(A)(i) by encouraging users to sign up for subscriptions and thereby using the data for commercial use , meaning Anna's Archive receives a fee for a service relying on WorldCat data. Terms and Conditions, Dkt. 1-2 at PageID 46; *see also id.* at PageID 47(defining "Commercial Use" as the use of the data "as part of or to facilitate a service for which You receive a fee"); Compl. ¶¶ 72–73; Rozek Decl. ¶ 32.

OCLC properly alleges the other contractual breach elements. The Terms and Conditions is a valid and binding contract. When Anna's Archive went to WorldCat.org to hack, scrape, and harvest, it became a "user" of WorldCat.org and agreed to the Terms and Conditions in exchange for a limited-use license from OCLC. Rozek Decl. ¶¶ 31, 32. OCLC provided Anna's Archive this limited-use license and access to WorldCat.org, thus fully performing its obligations under the Terms and Conditions. Compl. ¶¶ 77, 86, 124; Rozek Decl. ¶ 32; Murphy Decl. ¶ 10. And as set forth in its Motion, OCLC suffered immediate and irreparable injury and incurred damages. Mot., Dkt. 40 at PageID 761–71; *see also* Compl. ¶¶ 9, 81, 83–85, 100–104, 126–127; Murphy Decl. ¶ 12; Rozek Decl. ¶ 44.

Unjust Enrichment. OCLC's allegations also plead an unjust enrichment claim. *See Bunta v. Superior VacuPress, LLC*, 218 N.E.3d 838, 848 (Ohio 2022) (an unjust enrichment claim "requires a showing that (1) a benefit was conferred by the plaintiff on the defendant, (2) the defendant had knowledge of the benefit, and (3) the defendant retained the benefit under circumstances in which it was unjust to do so without payment."). Courts have recognized unjust enrichment claims in connection with data scraping or harvesting. *E.g.*, *Digital Drilling Data Sys., L.L.C. v. Petrolink Servs., Inc.*, 965 F.3d 365, 379–80, 382 (5th Cir. 2020); *Meta Platforms, Inc., v. Ekrem ATES*, No. 22-cv-03918-TSH, 2023 WL 4035611, at *6 (N.D. Cal. May 1, 2023).

Here, OCLC conferred a benefit on Anna's Archive when it offered access to WorldCat.org and certain public WorldCat data. Compl. ¶¶ 77, 86, 129; Murphy Decl. ¶ 10. Anna's Archive also knew of this benefit—expressly acknowledging how valuable WorldCat data is in a blog post and thanking OCLC for its work. Compl. ¶¶ 13, 130; Rozek Decl. ¶ 42. Additionally, OCLC has alleged that it would be unjust for Anna's Archive to retain the benefit of the WorldCat data because Anna's Archive not only avoided paying for a membership, which would have granted it

access to the WorldCat data it improperly obtained, but Anna's Archive is also offering others access to the data who are not WorldCat subscribers. Compl. ¶¶ 86, 93, 131; Murphy Decl. ¶ 14. There is also no real question whether Anna's Archive has unjustly retained the benefit of OCLC's WorldCat.org data, as Anna's Archive acted in bad faith by exploiting its access to WorldCat data—which it admitted is proprietary—with the specific intent to hack OCLC, scrape data, and give it away for "free" to Anna's Archive's subscribers. Compl. ¶¶ 10, 12, 70, 86, 90, 132; Murphy Decl. ¶ 14.

Tortious Interference. OCLC's Complaint states claims for tortious interference with a contract and with prospective business relationships. *Fred Siegel Co., LPA v. Arter & Hadden*, 707 N.E.2d 853, 858 (Ohio 1999) (stating the elements of a claim for tortious interference with contract "are (1) the existence of a contract, (2) the wrongdoer's knowledge of the contract, (3) the wrongdoer's intentional procurement of the contract's breach, (4) the lack of justification, and (5) resulting damages."); *Ga.-Pac. Consumer Prods. LP v. Four-U-Packaging, Inc.*, 701 F.3d 1093, 1102 (6th Cir. 2012) (explaining that "[t]he elements of a claim for tortious interference with business relationships are almost identical," the distinguishing factor being that the first element requires a prospective contractual relationship).

OCLC's allegations are sufficient to establish Anna's Archive's liability for tortious interference. First, OCLC has adequately pled the existence of contracts and prospective business relationships. OCLC has current contractual relationships with its WorldCat customers and member libraries, and OCLC has prospective business relationships with potential customers seeking cataloging record services. Compl. ¶¶ 136, 152.

Second, Anna's Archive knew of OCLC's contracts and relationships. OCLC specifically pled that Anna's Archive knew about these relationships, publicly acknowledged that WorldCat

data is proprietary, and knew that data it stole is not available for mass download without a subscription and certain data is not publicly available on WorldCat.org. *Id.* ¶¶ 90, 114, 137, 153; Murphy Decl. ¶ 14.

Third, Anna's Archive's interference is intentional. Interference is intentional if the defendant (1) "acted with the purpose or desire to interfere with the performance of the contract" or (2) "knew that interference was certain or substantially certain to occur as a result of its actions." *Horter Invest. Mgmt. LLC v. Cutter*, 257 F. Supp. 3d 892, 924 (S.D. Ohio 2017) (citation omitted). When Anna's Archive hacked WorldCat.org and OCLC's servers to scrape and distribute WorldCat data for free, Anna's Archive was, *at a minimum*, substantially certain that OCLC would face material difficulties in fulfilling its obligations under applicable agreements with its customers and members. Compl. ¶¶ 118, 138; Murphy Decl. ¶ 14. When Anna's Archive—a sophisticated pirate library—hacked OCLC's systems and servers and began to scrape and harvest large volumes of data, it was substantially certain that it would impede OCLC's ability to operate, which made it difficult for OCLC to provide services to its customers. *See* Compl. ¶¶ 80–85, 138. Further, by widely distributing the pirated data, Anna's Archive was substantially certain that current or future OCLC customers would choose to cancel memberships or forego joining OCLC's cooperative or paying for OCLC data since libraries could obtain the misappropriated data for free from Anna's Archive. *Id.* ¶¶ 70, 138, 154.

Finally, Anna's Archive's scraping lacks legitimate justification. *See Havensure, LLC v. Prudential Ins. Co. of Am.*, 595 F.3d 312, 315–16 (6th Cir. 2010) (listing the factors Ohio courts consider to determine if a defendant's interference lacks justification). Anna's Actions directly harmed OCLC and violated the Terms and Conditions. *E.g.*, Compl. ¶¶ 14, 125–27. What is more, Anna's Archive acted with improper, illegal motives—to promote the piracy of literary works and

OCLC's WorldCat data, and to directly hack OCLC's servers and hijack user credentials.[4] *Id.* ¶¶ 70, 86, 90, 139, 155.

Ohio Revised Code § 2913.04. OCLC establishes a statutory violation under Ohio Revised Code § 2913.04. Section 2913.04 criminalizes unauthorized use of "computer property" and improper access to "computer property." Under § 2913.04(B), "[n]o person, in any manner and by any means, including, but not limited to, computer hacking, shall knowingly gain access to . . . or cause access to be gained to any computer, computer system, computer network . . . without the consent of, or beyond the express or implied consent of, the owner of the computer, computer system, [or] computer network[.]" Ohio Revised Code § 2307.60(A)(1) creates a civil cause of action for damages resulting from any criminal act—including acts under § 2913.04.[5] *See Key Realty Ltd. v. Hall*, 173 N.E.3d 831, 857–58 (Ohio Ct. App. 2021).

Anna's Archive's hacking, scraping, and harvesting of WorldCat data is "computer hacking" as broadly defined under the Ohio statute. "Computer hacking" includes any "intentional use of a computer, computer system, or computer network in a manner that exceeds" the owner's permission. Ohio Rev. Code § 2913.01. Anna's Archive "gained access" to OCLC's computer network and systems when it hacked WorldCat.org and scraped and harvested WorldCat data and accessed OCLC's servers. *Id.* § 2913.01(T) (defining "gain access" to include retrieving data from, or otherwise making use of any resources of a computer, computer system, or computer network); Compl. ¶ 169. Anna's Archive went behind the public user interface and accessed OCLC's servers to harvest and scrape its data. Compl. ¶¶ 76–79; Murphy Decl. ¶ 10. And as set forth above, this

[4] The monetary and irreparable harms suffered by OCLC from Anna's Archive's conduct is detailed in OCLC's Memorandum in Support of its Motion for Default Judgment (Dkt. 40).
[5] Proof of an underlying criminal conviction is not required under § 2307.60. *Key Realty*, 173 N.E.3d at 857–58.

"access" went beyond OCLC's consent outlined in the Terms and Conditions. Compl. ¶¶ 76–79, 170. Additionally, Anna's Archive obtained a member library's credentials to access OCLC's subscription-based service and harvest WorldCat records directly from the servers. *Id.* ¶ 79; Murphy Decl. ¶ 10. All these actions constitute "computer hacking" that give rise to liability under § 2913.04(B).

Trespass to Chattels. OCLC also states a claim for trespass to chattel. A trespass to chattel may be committed by intentionally "using or intermeddling with a chattel in the possession of another." *Mercer v. Halmbacher*, 44 N.E.3d 1011, 1017 (Ohio Ct. App. 2015). A plaintiff has a possessory interest in their computer system and networks, such that intermeddling with those systems and networks via transmission of electronic signals that burden the efficiency of those systems support a trespass cause of action. *See CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021–22 (S.D. Ohio 1997). A trespass occurs when a party's use exceeds the limits of consent to use. *See eBay, Inc.*, 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000); *CouponCabin, LLC v. Savings.com, Inc.*, No. 2-14-CV-39-TLS, 2017 WL 83337, at *3 (N.D. Ind. Jan. 10, 2017) (holding a trespass to chattels claim was sufficiently alleged where "[d]efendants circumvented the Plaintiff's security measures once it had blocked their access in order to engage in data scraping-related activities").

Here, Anna's Archive intentionally intermeddled with OCLC's data, computer systems and networks when it hacked and scraped the data from WorldCat.org and OCLC's servers beyond the limits imposed by the Terms and Conditions. Compl. ¶¶ 85–86, 90, 184. Anna's Archive intermeddled with OCLC's proprietary data when it used and accessed the WorldCat data and made the data publicly available for download on its website. *Id.* ¶¶ 86, 90, 185. Anna's Archive's trespass on the data, computer systems, and networks impaired the "condition, quality, or value"

of OCLC's data, computer systems, and networks. *See CompuServe Inc.*, 962 F. Supp. at 1022 (holding that defendant's use of plaintiff's servers diminished the value of plaintiff's computer equipment by draining the computers' processing power and harmed plaintiff's reputation with customers); *Snap-on Bus. Sols. Inc. v. O'Neil & Assocs., Inc.*, 708 F. Supp. 2d 669, 678–80 (N.D. Ohio 2010) (finding defendant's potentially unauthorized access to plaintiff's servers impaired the servers' condition, quality, or value as the scraper program crashed the website and caused slow run times).

Even further, Anna's Archive's intermeddling materially and physically damaged OCLC's servers and infrastructure. For instance, these attacks substantially affected the performance of OCLC's systems and servers, requiring around-the-clock efforts from November 2022 to March 2023 to prevent services outages and maintain the production systems' performance for customers. Compl. ¶ 81; Murphy Decl. ¶ 12. Nevertheless, OCLC's customers experienced significant disruptions to service due to the attacks. Compl. ¶ 82; Rozek Decl. ¶ 56; Murphy Decl. ¶ 12. OCLC suffered immediate and irreparable injury and incurred damages. Mot., Dkt. 40 at PageID 761–71; *see also, e.g.*, Compl.¶¶ 9, 81, 83–86, 90, 100–104, 126–127, 185.

Conversion. OCLC's well-pled allegations also support a conversion claim. *Bush v. Signals Power & Grounding Specialists, Inc.*, No. 08 CA 88, 2009 WL 3087202, at *2 (Ohio Ct. App. Sept. 25, 2019) (noting the elements of conversion are "(1) a defendant's exercise of dominion or control; (2) over a plaintiff's property; and (3) in a manner inconsistent with the plaintiff's rights of ownership."). Under Ohio Law, "identifiable intangible property rights," such as domain names, emails, and computer programs, may be subject to conversion, meaning OCLC has property rights in its WorldCat data. *See Eysoldt v. ProScan Imaging*, 957 N.E.2d 780, 786 (Ohio Ct. App. 2011).

Anna's Archive exercised control and dominion over the WorldCat data when it scraped, harvested, and distributed the data through its website. Compl. ¶¶ 90, 93, 200. The WorldCat data and compilation of the WorldCat data was created by OCLC, and only existed, in bulk, by purchasing a subscription. *Id.* ¶¶ 29, 44, 52, 199; Rozek Decl. ¶ 15. Moreover, Anna's Archive acted inconsistently with OCLC's rights over the data by unlawfully acquiring WorldCat data in violation of OCLC's Terms and Conditions. Compl. ¶¶ 58, 125, 202.

Although Ohio courts have not addressed a conversion claim involving hacking, harvesting, or scraping, other courts have recognized such claims in comparable contexts. *See In re Clearview AI, Inc. Consumer Priv. Litig.*, 585 F. Supp. 3d 1111, 1127–28 (N.D. Ill. 2022) (holding plaintiffs sufficiently pled conversion where they alleged "defendants scraped their images in violation of the terms of service of the websites on which their images were hosted and without the plaintiffs' consent"); *Integrated Direct Mktg., LLC v. May*, 143 F. Supp. 3d 418, 428 (E.D. Va. 2015) (finding a conversion claim viable where the defendant copied electronic files containing confidential and proprietary information).

Civil Conspiracy. OCLC adequately pleads five separate civil conspiracy claims against Anna's Archive based on the underlying claims of tortious interference of contract, tortious interference of prospective business relationships, violations of § 2913.04, trespass to chattels, and conversion. To establish a claim for civil conspiracy in Ohio, a plaintiff must allege "(1) a malicious combination, (2) two or more persons, (3) injury to person or property, and (4) the existence of an unlawful act independent from the actual conspiracy." *Aetna Cas. & Sur. Co. v. Leahey Constr. Co.*, 219 F.3d 519, 534 (6th Cir. 2000) (citations omitted). Courts have found civil conspiracy claims will lie in internet and data-scraping contexts. *See Key Realty*, 173 N.E.3d at 862 (using social media website); *DHI Grp., Inc. v. Kent*, No. H-16-1670, 2017 WL 9939568, at

*4, 9 (S.D. Tex. Apr. 27, 2017) (holding that plaintiff sufficiently pled civil conspiracy where there was an agreement for defendants to work in concert to scrape online job boards, including resume databases, to look for "backdoors").

The allegations in the Complaint support liability for civil conspiracy. Anna's Archive formed a malicious combination to hack OCLC's computer servers and WorldCat.org, to scrape and harvest WorldCat data, and to distribute WorldCat data; these were Anna's Archive's stated objectives. Compl. ¶¶ 15, 90, 118, 145–146, 162–163, 176–177, 192–193, 208–209. Put differently, OCLC's Complaint illustrates that Anna's Archive had "a common understanding or design, even if tacit", to commit the "unlawful act[s]." *Woodward Const., Inc. v. For 1031 Summit Woods, LLC*, 30 N.E.3d 237, 243 (Ohio Ct. App. 2015). Anna's Archive's blog posts, as described and incorporated in the Complaint, demonstrate Anna's Archive and the individuals who run it had a plan to act in concert with one another to hack and scrape the WorldCat data, stating "we set our sights on . . . WorldCat" and "[o]ver the past year, we've meticulously scraped all WorldCat records." Compl. ¶¶ 15, 86.

OCLC adequately alleges the remaining elements. Anna's Archive's blog posts continuously refer to more than one individual being behind Anna's Archive; OCLC has experienced harm; and OCLC has several claims, also set forth above, which include acts that are independent from the actual conspiracy. *Id.* ¶¶ 15, 118, 143–144, 160–161, 175, 191, 207.

IV. Conclusion

For the aforementioned reasons, paired with the reasons set forth in OCLC's Motion for Default Judgment, OCLC respectfully prays that a default judgment be entered in its favor and against Defendant Anna's Archive on each of the claims in its Complaint for the requested

declaratory, injunctive, and monetary relief. To the extent questions remain, OCLC respectfully requests a status conference or a hearing to address the Court's further questions.

Respectfully submitted,

/s/ Jeffrey M. Walker
Jeffrey M. Walker (0096567), Trial Attorney
Traci L. Martinez (0083989)
Kathryn M. Brown (0100426)
Brittany N. Silverman (0102263)
SQUIRE PATTON BOGGS (US) LLP
2000 Huntington Center
41 South High Street
Columbus, Ohio 43215
Telephone: +1 614 365 2700
Fax: +1 614 365 2499
jeffrey.walker@squirepb.com
traci.martinez@squirepb.com
kathryn.brown@squirepb.com
brittany.silverman@squirepb.com

Attorneys for Plaintiff OCLC, Inc.

CERTIFICATE OF SERVICE

On October 22, 2024, this document and the accompanying attachment was filed electronically with the Clerk of the United States District Court for the Southern District of Ohio, Eastern Division, which will electronically serve a copy of the foregoing on all counsel of record for all parties, and will be served upon Anna's Archive at the following email addresses:

AnnaArchivist@proton.me
AnnaDMCA@proton.me
AnnaArchivist+security@proton.me
domainabuse@tucows.com

/s/ Jeffrey M. Walker
Jeffrey M. Walker

An Attorney for Plaintiff OCLC, Inc.